



Windows 2000 Kernel Security Status

03 November 2000

**Clyde Wurster
Defense Information Systems
Agency
DII COE Engineering Office
(703) 735-8507
wursterc@ncr.disa.mil**



Overview

- **There are significant security vulnerabilities in the OS**
- **The kernel is not fully locked down out of the box- W2K resets the NT lockdown to the W2K defaults i.e. everyone group, power users**
- **Windows 2000 integration problems**
 - **Problems with upgrade path from NT**
 - **NT-Windows 2000 domain integration problems**
- **New security features not addressed**

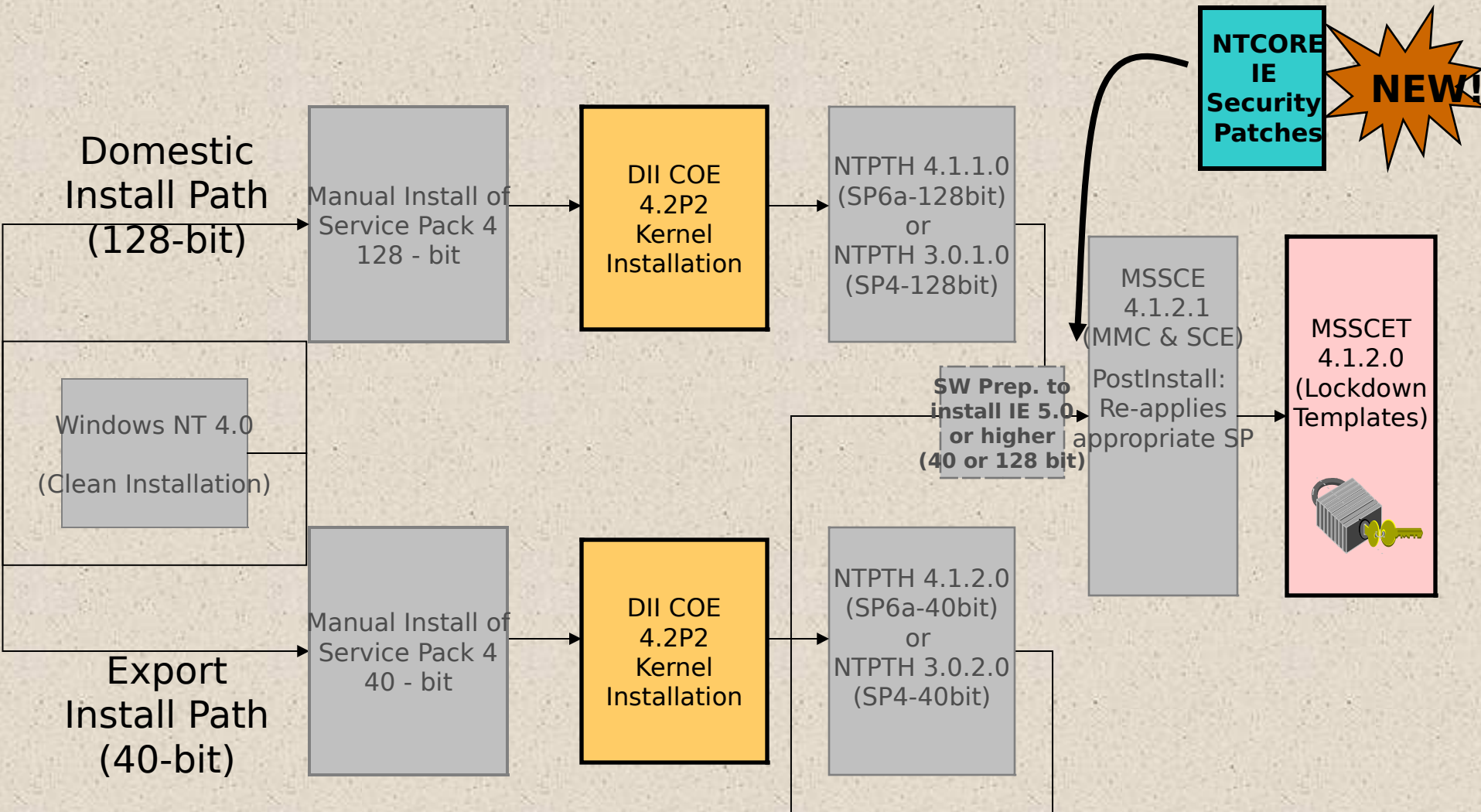


W2K Security Vulnerabilities

- Microsoft has currently released 21 security patches for Windows 2000
- Of the 21 security patches, only 9 are included in SP1
- In the past 2 months, Microsoft has released 7 security patches for Windows 2000
- An average of 3 new security vulnerabilities a month can be expected
- All available security patches will be included with W2KPTH



NT Installation Sequence



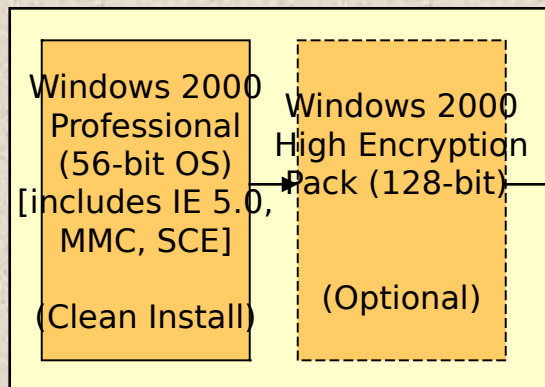


W2K Kernel Security Lockdown Status

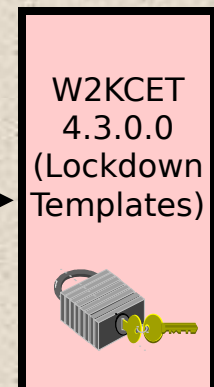
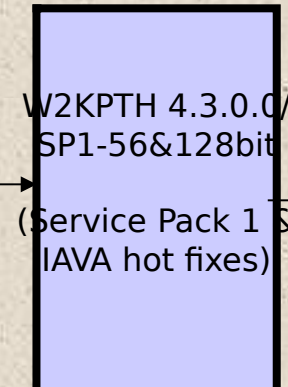
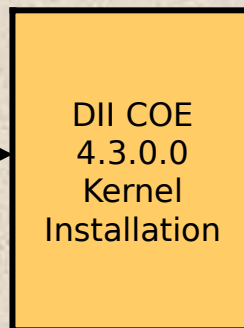
COE 4.3 - Windows 2000 Installation Sequence

Minimal security applied by kernel at this time


W2K Lockdown Templates



Windows 2000 product package



Security templates are under development

 = manual / non-segmented process



W2K Integration Problems

- Default (non-secure) filesystem and registry settings are reset upon upgrade from NT
- PDC-BDC communication in mixed NT-W2K environments has “lost” information
 - Windows loses information between the PDC/BDC and a W2K DC during communications, based on research not actual experience



New Security Features in

- **Active Directory-** is a **W2K** hierarchical namespace that allows Organizational Units (OU). OUs can inherit security policies from higher OUs (NT 4.0 uses a flat namespace) - W2K will automatically establish an Active Directory structure during installation - same as Novell's NDS
- **Kerberos-** used as default authentication protocol
 - Use lowest authentication level
- **Smart Cards-** can be used for authentication (Don't Implement)
- **IPSec-** provides data integrity, confidentiality, and authentication. (Don't Implement)



New Security Features in

W2K

- Virtual Private Networks (VPN)- enables a user to tunnel through the internet or another public network, while maintaining the same level of security that would be provided by a private network. (Don't Implement)
- Transitive Two-Way Trust- The Windows 2000 hierarchical domain tree allows users with accounts defined in one domain to be authenticated by resource servers in another domain. (Still Exploring)



New Security Features in W2K

- **Delegating Administration-** Administration can be defined by subsets or to an entire organizational domain. will allow better access control rights giving the ability to grant rights for resetting passwords, created user account, editing user properties, etc. (Need to define Administrative Roles)
- **Access Control List-** Greater granularity, and more control.



Priority for Defining Security

- Workstations, Domains, Servers for W2K
- Kerberos
- Access Control List
- Transitive Two-Way Trust
- Active Directory
- Delegating Administration
- IPSec
- Virtual Private Networks (VPN)
- Smart Cards



Status of W2K Security Vulnerabilities and Features

- More than half the current security vulnerabilities are not covered by SP1
- Active Directory, in particular, needs to be carefully reviewed and managed. Unrestricted permission settings could jeopardize the security of every organizational domain.
- New security features should be carefully evaluated and protected from unrestricted access as necessary



Conclusion

- December release of NSA security guide for W2K can be used as security baseline
- Subsequent security enhancements made through security template & patch segments